REMARKS/ARGUMENTS

In the Office Action dated September 22, 2011 (hereinafter, "Office Action"), claims 1-20 were rejected under 35 U.S.C. § 103(a). By this paper, claims 1, 13, 15 and 18 are being amended. Claims 11-12 are being canceled.

Applicant respectfully responds to the Office Action.

I. Claims 1-3, 5-6 and 8-20 Rejected Under 35 U.S.C. § 103(a)

Claims 1-3, 5-6 and 8-20 stand rejected under 35 U.S.C. § 103(a) based on U.S. Patent No. 7,647,402 to McBrearty et al. (hereinafter, "McBrearty") in view of U.S. Patent Application Publication No. 2004/0123150 to Wright et al. (hereinafter, "Wright"). Applicant respectfully requests reconsideration in view of the above claim amendments and the following remarks.

The factual inquiries that are relevant in the determination of obviousness are determining the scope and contents of the prior art, ascertaining the differences between the prior art and the claims in issue, resolving the level of ordinary skill in the art, and evaluating evidence of secondary consideration. KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 406 (2007) (citing Graham v. John Deere Co. of Kansas City, 383 U.S. 1, 17-18 (1966)). As the Board of Patent Appeals and Interferences has recently confirmed, "obviousness requires a suggestion of all limitations in a claim." In re Wada and Murphy, Appeal 2007-3733 (citing CFMT, Inc. v. Yieldup Intern. Corp., 349 F.3d 1333, 1342 (Fed. Cir. 2003)).

Independent claim 1 has been amended to recite "access[ing] sensitive file information which identifies multiple sensitive files stored on the computing device, ... wherein the sensitive file information is separate from the sensitive files." Support for this claim subject matter is found in at least Figures 1, 5-6 and in paragraphs [0044] and [0053]-[0054] of the filed specification. Applicant respectfully submits that the combination of McBrearty and Wright does not teach or suggest "access[ing] sensitive file information which identifies multiple sensitive files stored on the computing device, ... wherein the sensitive file information is separate from the sensitive files," because the cited reference (McBrearty) indicates that a user is checked against an authorized list to determine if the user should have access to the file, but does not teach or suggest that there is separate sensitive file information that identifies the sensitive files. McBrearty teaches "a system, method and program for protecting data files from being stolen or compromised." (McBrearty, col. 2, lines 46-48.) Specifically, "[w]hen a user requests a file ... a determination is made ... as to whether the user is authenticated, i.e. his ID matches the ID of [an] authorized user," and "[i]f Yes, the user is granted access to the requested file" and "[i]f No, then the user is refused access to the file." (McBrearty, col. 5, lines 58-63.) If there are repeated failures at authorization for the specific file, the system determines that there is a potential intruder trying to access the file. (See McBrearty, col. 4, lines 35-43.) Other ways for determining that a hacker is trying to access the file may also be used. (See McBrearty, col. 6, lines 4-7.) After this potential intrusion is determined, the "target file is renamed" with a name that does not give "information about the contents of the file," and the "whole file is then moved ... to another hidden or covert directory." (McBrearty, col. 6, lines 10-16.) "In this manner, the hacker attacking the files is still continuing to look for the original file which has been renamed, hidden in a different directory and, thus, protected." (McBrearty, col. 4, lines 49-51.)

As best understood, the Office Action cites to McBrearty's determining whether a "user ID" matches an ID in the authorized list as constituting the claimed "accessing sensitive file information." (See, e.g., Office Action, page 3 (indicating that the sensitive file list involves "check[ing]" a requester "against an authorized list").) However, determining whether a user ID matches an ID in an authorized list does not constitute accessing sensitive file information that "identifies multiple sensitive files stored on the computing device" and that this information is separate from the sensitive files. The user ID list of McBrearty contains a list of authorized user IDs, and does not list or indicate which files are sensitive and that such listing of files is separate from the sensitive files. Moreover, comparing a user ID with a user ID list does not indicate that sensitive file information is "accessed." For this reason, McBrearty does not teach or suggest "access[ing] sensitive file information which identifies multiple sensitive files stored on the computing device, ... wherein the sensitive file information is separate from the sensitive files," as recited by amended claim 1.

Further, claim 1 has also been amended to recite "accessing an authorized connection list, wherein the authorized connection list comprises a list of at least one authorized network or a list of at least one authorized connection type." Support for this claim subject matter is found in originally-filed claims 11-12. Thus, as taught by claim 1, the authorized connection list (which is different from the sensitive file information) comprises "a list of at least one authorized network or a list of at least one authorized connection type."

Applicant respectfully submits that the combination of McBrearty and Wright does not teach or suggest "accessing an authorized connection list, wherein the authorized connection list comprises a list of at least one authorized network or a list of at least one authorized connection type" because the cited reference (McBrearty) does not indicate that the authorized connection list is either a list of authorized networks (such as, for example, wireless networks, etc.) or a list of authorized connection types (such as, for example, Ethernet, LAN, etc.). The Office Action indicates that "McBrearty, Col 3, Line 64 thru Col 4, Line 11" allegedly teaches determining a network type such as an "internet web connection." (See Office Action, page 5.) However, this section of McBrearty states:

> However, many databases may be accessed over the Web and the present invention is intended to protect such Web sites and databases in the manner which we will describe with respect to Web site or Internet station 57. This station is connected to the Web through connection 51 and Web server 53 which includes firewall 52. Thus, files may be requested by users at stations such as Web station 57 including computer 56 throughout the Web 50 or requests for files may come from users at IP locations such as addresses 63 and 65. Such requests are processed to the particular database through the respective Web station server 53. Each server has the means for processing such requests, including authenticating the user IDs and then determining whether such identified users have authorizations for particular data file access to be hereinafter described.

McBrearty, col. 3, line 64-col. 4, line 11. Thus, this section of McBrearty indicates that files on a computer may be requested by other computers through the Internet, but the user ID will be checked before access to the requested files is granted. (See id.) To the extent that McBrearty teaches that files may be accessed through the Internet, this teaching does not indicate that there is an authorized connection list that details which networks or connection types are authorized. Rather, the fact that a user ID is checked against a database simply teaches that a list of authorized user IDs is kept, not that there is a list of authorized networks and connection types. Moreover, it appears that the Office Action is asserting that the action of looking up whether a user ID is found in a list of authorized user IDs constitutes both the operation of "accessing sensitive file information" and accessing an authorized "connection list." Such an interpretation is improper because the sensitive file information is different from the authorized connection list, and thus, looking up a user ID in the same database cannot satisfy both of these claimed tasks. For this reason, McBrearty does not teach or suggest "accessing an authorized connection list, wherein the authorized connection list comprises a list of at least one authorized network or a list of at least one authorized connection type," as recited by amended claim 1.

With respect to Wright, this reference is again cited as teaching "hiding ... all sensitive data when an unauthorized connection/location is detected." (Office Action, page 3.) However, teaching that all of the sensitive files are hidden when there is an intruder does not teach or suggest "accessing an authorized connection list, wherein the authorized connection list comprises a list of at least one authorized network or a list of at least one authorized connection type." Thus, Wright does not make up for the deficiencies of McBrearty.

For at least the foregoing reasons, Applicant respectfully submits that amended claim 1 is allowable over Wright and McBrearty. Claims 2-3, 5-6 and 8-10 depend from claim 1, and are therefore allowable for at least the same reasons as claim 1. Claims 11-12 are being canceled.

Amended claim 13 recites "access[ing] an authorized connection list, wherein the authorized connection list comprises a list of at least one authorized network or a list of at least one authorized connection type." As discussed above, the combination of McBrearty and Wright does not teach or suggest this claimed subject matter. Claim 13 further recites "access[ing] sensitive file information which identifies multiple sensitive files stored on the computing device, ... wherein the sensitive file information is separate from the sensitive files." As discussed above, this claim subject matter is also not taught or suggested by McBrearty and Wright. Accordingly, Applicant respectfully submits that amended claim 13 is allowable. Claim 14 depends from claim 13, and is therefore allowable for at least the same reasons as claim 13.

Amended claim 15 recites "access[ing] an authorized connection list, wherein the authorized connection list comprises a list of at least one authorized network or a list of at least one authorized connection type." As discussed above, the combination of McBrearty and Wright does not teach or suggest this claimed subject matter. Claim 15 further recites "access[ing] sensitive file information which identifies multiple sensitive files stored on the computing device, ... wherein the sensitive file information is separate from the sensitive files." As discussed above, this claim subject matter is also not taught or suggested by McBrearty and Wright. Accordingly, Applicant respectfully submits that amended claim 15 is allowable. Claims 16-17 depend from claim 15, and are therefore allowable for at least the same reasons as claim 15.

Amended claim 18 recites "access[ing] an authorized connection list, wherein the authorized connection list comprises a list of at least one authorized network or a list of at least one authorized connection type." As discussed above, the combination of McBrearty and Wright does not teach or suggest this claimed subject matter. Claim 18 further recites "access[ing] sensitive file information which identifies multiple sensitive files stored on the computing device, ... wherein the sensitive file information is separate from the sensitive files." As discussed above, the combination of McBrearty and Wright does not teach or suggest this claimed subject matter. Accordingly, Applicant respectfully submits that amended claim 18 is allowable. Claims 19-20 depend from claim 18, and are therefore allowable for at least the same reasons as claim 18.

II. Claim 4 Rejected Under 35 U.S.C. § 103(a)

Claim 4 stands rejected under 35 U.S.C. § 103(a) based on McBrearty and Wright and further in view of U.S. Patent Application Publication No. 2003/0056095 to Elliott et al. (hereinafter, "Elliott"). Applicant respectfully requests reconsideration in view of the above claim amendments and the following remarks.

Claim 4 depends from claim 1. As discussed above, Applicant respectfully submits that claim 1 is allowable. Accordingly, Applicant respectfully submits that claim 4 is allowable for at least the same reasons as presented above in connection with claim 1.

III. Claim 7 Rejected Under 35 U.S.C. § 103(a)

Claim 7 stands rejected under 35 U.S.C. § 103(a) based on McBrearty and Wright and further in view of U.S. Patent No. 5,265,159 to Kung (hereinafter, "Kung"). Applicant respectfully requests reconsideration in view of the above claim amendments and the following remarks.

Claim 7 depends from claim 1. As discussed above, Applicant respectfully submits that claim 1 is allowable. Accordingly, Applicant respectfully submits that claim 7 is allowable for at least the same reasons as presented above in connection with claim 1.

CONCLUSION

In view of the foregoing, Applicant respectfully submits that all pending claims in the present application are in a condition for allowance, which is earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

/Wesley L. Austin/

Wesley L. Austin
Reg. No. 42,273
Attorney for Applicant

Date: December 22, 2011

AUSTIN RAPP & HARDMAN
170 South Main Street, Suite 735
Salt Lake City, Utah 84101
Telephone: (801) 537-1700

12/22/2011